



Provisioning Management VPN

This chapter describes how to implement the IP Solutions Center (ISC) Management VPN. This chapter contains the following major sections:

- [Overview of the ISC Management Network, page 9-1](#)
- [Provisioning a Management CE in ISC, page 9-7](#)

Overview of the ISC Management Network

This section provides the fundamental concepts and considerations for administering customer edge routers (CEs) in the context of an ISC management subnet. Before ISC can be appropriately deployed to deliver services to customers, the question of whether the CEs are to be managed by the Service Provider or not must be answered

This section contains the following sections:

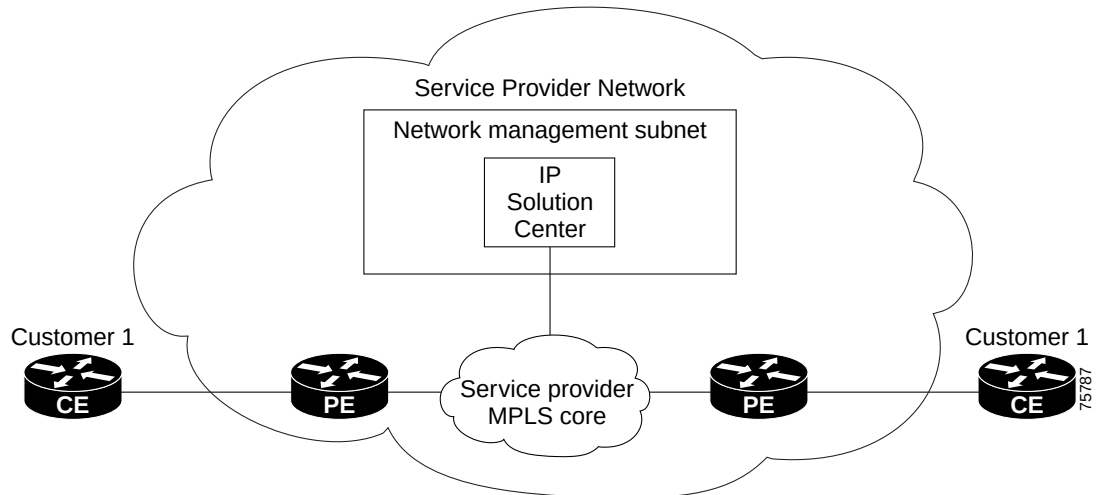
- [Unmanaged Customer Edge Routers, page 9-1](#)
- [Managed Customer Edge Routers, page 9-2](#)
- [Network Management Subnets, page 9-3](#)
- [Implementation Techniques, page 9-4](#)
- [Out-of-Band Technique, page 9-7](#)

Unmanaged Customer Edge Routers

One of the options available to the Service Provider is to not manage the customer edge routers (CEs) connected to the Service Provider network. For the Service Provider, the primary advantage of an unmanaged CE is administrative simplicity.

If the CEs are unmanaged, the provider can use IPv4 connectivity for all management traffic. ISC is not employed for provisioning or managing unmanaged CEs.

[Figure 9-1](#) shows a basic topology with unmanaged CEs. The network management subnet has a direct link to the Service Provider MPLS core network.

Figure 9-1 Service Provider Network and Unmanaged CEs

Regarding unmanaged CEs, Service Providers should note the following considerations:

- Because unmanaged CEs are outside the Service Provider's administrative domain, the Service Provider does not maintain or configure unmanaged CEs.
- The Service Provider does *not* administer the following elements on the unmanaged CE:
 - IP addresses
 - Host name
 - Domain Name server
 - Fault management (and timestamp coordination by means of the Network Time Protocol)
 - Collecting, archiving, and restoring CE configurations
 - Access data such as passwords and SNMP strings on the unmanaged CE
- Prototype CE configlets are generated, but they are not automatically downloaded to the router.
- There is no configuration management.
 - With no configuration management, no configuration history is maintained and there is no configuration change management.
 - Changes to a service request (on the PE-CE link) are not deployed to the CE.
- There is no configuration auditing because there is no means to retrieve the current CE configuration.
- You can perform routing auditing.
- You can use the Service Assurance Agent (SA Agent) to measure response times between shadow routers, but you *cannot* use SA Agent to measure response times between CEs.

Managed Customer Edge Routers

The alternative to unmanaged CEs is managed CEs, that is, customer edge routers managed by the Service Provider. Managed CEs can be wholly within the Service Provider's administrative domain or co-managed between the provider and the customer, although CE co-management poses a number of ongoing administrative challenges and is not recommended.

Regarding managed CEs, Service Providers should note the following considerations:

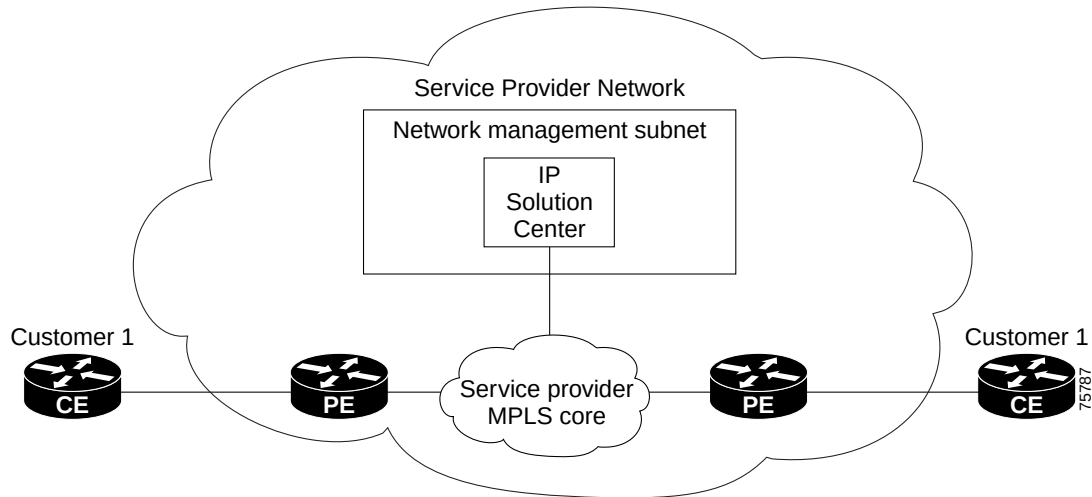
- Managed CEs are within the Service Provider's administrative domain. Thus, some connectivity to the CEs from the Service Provider network is required.
- The Service Provider must administer the following elements on the managed CE:
 - IP addresses
 - Host name
 - Domain Name server
 - Access data such as passwords and SNMP strings
- The Service Provider should administer fault management (and timestamp coordination by means of the Network Time Protocol)
- The Service Provider can administer collecting, archiving, and restoring CE configurations.
- CE configlets are generated and downloaded to the managed CE.
- Changes to service requests are based on the current CE configuration and automatically downloaded.
- The CE configurations are audited.
- Customer routing and Service Provider routing must interact.
- Access from CEs to the management hosts on the network management subnet is required.
- Configuration auditing and routing auditing are both functional.
- You can use the Service Assurance Agent (SA Agent) to measure response times between CEs and between shadow routers.

The following sections discuss the concepts and issues required for administering a managed CE environment.

Network Management Subnets

The Network Management Subnet is required when the provider's service offering entails the management of CEs. Once a CE is in a VPN, it is no longer accessible by means of conventional IPv4 routing unless one of the techniques described in this chapter is employed.

[Figure 9-2](#) shows the ISC network management subnet and the devices that might be required to connect to it:

Figure 9-2 The ISC Network Management Subnet

Issues Regarding Access to VPNs

The core issues with regard to gaining access to VPNs are as follows:

- How to keep provider space “clean” from unnecessary customer routes
- How to keep customer space “clean” from both the provider’s and other customer’s routes
- How to provide effective security
- How to prevent routing loops

ISC does not handle any of these responsibilities—doing so must be designed and implemented by the Service Provider.

- Reachability changes as a direct consequence of employing ISC.

Before you provision a CE in the ISC, you might be able to reach the CE via IPv4 connectivity, but the moment the product deploys a service request, you cannot reach that CE any more—unless you have *first* implemented the network management subnet.

Implementation Techniques

The network management subnet must have access to a Management CE (MCE) and PEs.

The network management subnet is appropriate—and necessary—when there is an intent to have managed CEs connected via an in-band connection. *In-band* indicates a single link or permanent virtual circuit (PVC) that carries *both* the customer's VPN traffic, as well as the provider’s network management traffic.

Management CE (MCE)

The network management subnet is connected to the Management CE (MCE). The MCE *emulates* the role of a customer edge router (CE), but the MCE is in provider space and serves as a network operations center gateway router. The MCE is part of a management site as defined in the ISC.

You configure the MCE by identifying the CE as part of the management LAN in ISC.

Management PE (MPE)

The Management PE (MPE) *emulates* the role of a PE in the provider core network. The MPE connects the MCE to the provider core network. An MPE can have a dual role as both a PE and the MPE.

The MPE needs access to the following devices:

Device	Connectivity	Function
1. Customer Edge Routers (CEs)	Access from the network management subnet into the VPNs	Provision or change configuration and collect SA Agent performance data
2. Shadow CEs	Access from the network management subnet into the VPNs	A simulated CE used to measure data travel time between two devices. A shadow CE is connected directly to a PE via Ethernet.
3. Provider Edge Routers (PEs)	Standard IP connectivity	Provision or change configuration

At the current time, ISC recommends two main network management subnet implementation techniques:

- *Management VPN Technique*

The MPE-MCE link uses a Management VPN (see [Management VPN, page 9-5](#)) to connect to managed CEs. To connect to the PEs, the MPE-MCE link uses a parallel IPv4 link.

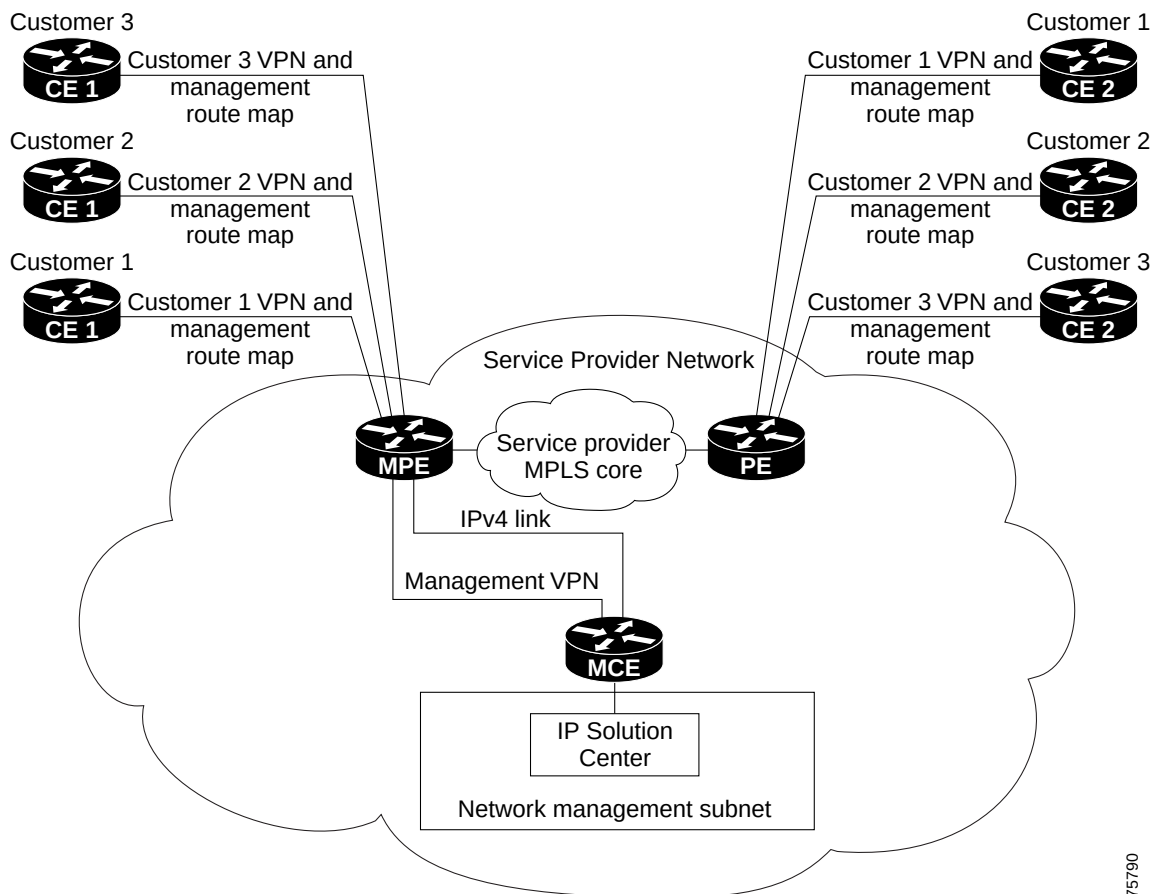
- *Out-of-Band Technique*

In the Out-of-Band technique, the MCE has IPv4 connectivity (that is, not MPLS VPN connectivity) to all the CEs and PEs in the network (see [Out-of-Band Technique, page 9-7](#)). In this context, *out-of-band* signifies a separate link between PEs that carries the provider's management traffic.

The network management subnet technique the provider chooses to implement depends on many factors, which are discussed later in this chapter.

Management VPN

The Management VPN technique is the default method provisioned by ISC. A key concept for this implementation technique is that *all the CEs in the network are a member of the management VPN*. To connect to the PEs, the MPE-MCE link uses a parallel IPv4 link. [Figure 9-3](#) shows a typical topology for the Management VPN technique.

Figure 9-3 Typical Topology for a Management VPN Network

When employing the Management VPN technique, the MPE-MCE link uses a *management VPN* to connect to managed CEs. To connect to the PEs, the MPE-MCE link employs a parallel IPv4 link.

Each CE in a customer VPN is also added to the management VPN by selecting the **Join the management VPN** option in the service request user interface.

The function of the management route map is to allow only the routes to the specific CE into the management VPN. The Cisco IOS supports only one export route map and one import route map per VRF.

As shown in [Figure 9-3](#), a second parallel non-MPLS VPN link is required between the MPE and MCE to reach the PEs.

**Note**

Implementation of the Management VPN technique requires Cisco IOS 12.07 or higher.

Advantages

The advantages involved in implementing the Management VPN technique are as follows:

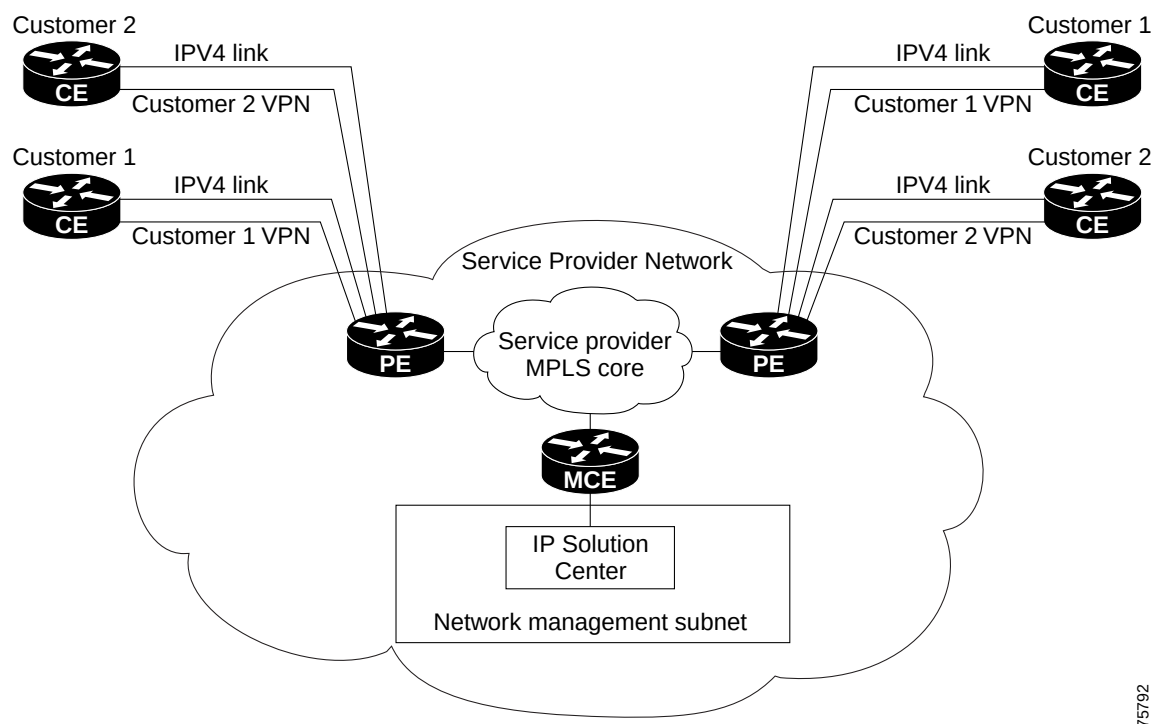
- Provisioning with this method requires only one service request.
- The only routes given to the network management subnet are the routes to the CEs—that is, either the address of the CE link to the PE or the CE loopback address. General VPN routes are *not* given to the network management subnet.

- A CE in the Management VPN method is a spoke to the Management VPN regardless of which role the CE has within its own VPN. Therefore, CEs cannot be accidentally exposed to inappropriate routes. The only management routes the CEs can learn must come from a hub of the Management VPN.

Out-of-Band Technique

The Out-of-Band technique does not employ a management VPN to manage the CEs. Out-of-band connectivity is provided by IPv4 links. *Out-of-band* signifies a separate link between PEs that carries the provider's management traffic. As shown in [Figure 9-4](#), the MCE provides separation between the provider's routes and the customer's routes.

Figure 9-4 Out-of-Band Technique



The Out-of-Band technique has the advantage of being relatively simple to set up, and no management VPN is required. However, its disadvantages are that it is expensive since it requires an IPv4 connection to each CE. Also, due to the delicate staging requirements for this technique, the Out-of-Band implementation does have a high degree of complexity.

Provisioning a Management CE in ISC

The ISC network management subnet is connected to the Management CE (MCE). The MCE *emulates* the role of a customer edge router (CE), but the MCE is in provider space and serves as a network operations center gateway router. The MCE is part of a management site as defined in ISC.

This section contains the following sections:

- [Defining a CE as an MCE, page 9-8](#)

- [Creating an MCE Service Request, page 9-9](#)

Defining a CE as an MCE

You configure the MCE by identifying the CE as part of the management LAN in ISC software. To define a CE as an MCE, follow these steps:

- Step 1** Start up and log in to ISC.
- Step 2** From the Welcome to ISC window, choose **Service Inventory**.
- Step 3** From the Service Inventory window, choose **Inventory and Connection Manager**.
- Step 4** From the TOC (table of contents) displayed on the left side of the Inventory and Connection Manager window, choose **CPE Devices**.

The list of CPE devices for all currently defined customers is displayed (see [Figure 9-5](#)).

Figure 9-5 List of All CPEs for All Customers

CPE Devices

Show CPEs with matching

Showing 1-10 of 14 records

#	☐	Device Name	Customer Name	Site Name	Management Type
1.	☐	mlce1.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
2.	☐	mlce2.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
3.	☐	mlce8.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
4.	☐	mlce9.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
5.	☐	mlsw3.cisco.com	AcmeInc	Acme_SF	Multi-VRF - No SA Agent
6.	☐	mlce12.cisco.com	AcmeInc	Acme_TX	Managed - No SA Agent
7.	☐	mlce13.cisco.com	AcmeInc	Acme_TX	Managed - No SA Agent
8.	☐	mlce3.cisco.com	WidgetsInc	Widgets_SF	Multi-VRF - No SA Agent
9.	☐	mlsw3CE.cisco.com	WidgetsInc	Widgets_SF	Managed - No SA Agent
10.	☐	mlce4.cisco.com	WidgetsInc	Widgets_NY	Managed - No SA Agent

Rows per page: << Page 1, 2 >>

- Step 5** Choose the CE that will function as the MCE in the management VPN, then click **Edit**.

The Edit CPE Device dialog box appears, displaying the pertinent information for the selected CPE (see [Figure 9-6](#)).

Figure 9-6 Editing the Selected CPE Device

Edit CPE Device

Device Name: mlce8.cisco.com
 Site Name: Acme_SF
 Customer Name: AcmeInc
 Management Type: Managed - Management LAN
 Wildcard Preshare Key:
 IP Address Ranges:

Showing 1-5 of 11 records

#	Name	IP Address	IP Address Type	Encapsulation	Description	IPsec	Firewall	NAT	QoS Candidate
1.	ATM3/0		STATIC	UNKNOWN		None	None	None	None
2.	ATM3/1		STATIC	UNKNOWN		None	None	None	None
3.	ATM3/2		STATIC	UNKNOWN		None	None	None	None
4.	FastEthernet0/0	172.29.146.31/26	STATIC	UNKNOWN	CONNECTION TO MLGW1 - DO NOT TOUCH	None	None	None	None
5.	FastEthernet0/1		STATIC	UNKNOWN	L7: Link To mls3	None	None	None	None

Rows per page: 5 << Page 1, 2, 3 >>

Step 6 *Management Type:* From the drop-down list, set the management type to **Managed—Management LAN**.

Step 7 Click **Save**.

You return to the list of CPE devices, where the new management type for the selected CE (in our example, 3. *mlce8.cisco.com*) is now displayed (see [Figure 9-7](#)).

Figure 9-7 Selected CE Defined as a Management CE

CPE Devices

Show CPEs with matching

Showing 1-5 of 14 records

#	☐	Device Name	Customer Name	Site Name	Management Type
1.	☐	mlce1.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
2.	☐	mlce2.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
3.	☐	mlce8.cisco.com	AcmeInc	Acme_SF	Managed - Management LAN
4.	☐	mlce9.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
5.	☐	mlsw3.cisco.com	AcmeInc	Acme_SF	Multi-VRF - No SA Agent

Creating an MCE Service Request

To create an MCE service request, follow these steps:

- Step 1** Start up and Log in to ISC.
- From the Welcome to ISC window, choose **Service Inventory**.

- b. From the Service Inventory window, choose **Inventory and Connection Manager**.
- c. From the Inventory and Connection Manager window, choose **Service Requests**.

The Service Requests dialog box appears (see [Figure 9-8](#)).

Figure 9-8 Initial Service Requests Dialog Box

Service Requests

Show Services with Job ID matching * of type All Find

Showing 0 of 0 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
---	--------	-------	------	----------------	---------	---------------	-------------	---------------	-------------

Rows per page: 10

Auto Refresh: ☒

Create Details Edit Deploy Decommission Purge

Step 2 To start the process to create a new service, click **Create**.

A drop-down list is displayed, showing the types of service requests you can create.

Step 3 Choose **MPLS VPN**.

The Select MPLS Policy dialog box appears (see [Figure 9-9](#)).

This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

Figure 9-9 Selecting the MPLS Policy for This Service

Select MPLS Policy

Show MPLS policies with Policy Name Matching * Find

Showing 1 - 2 of 2 records

#	Policy Name	Policy Owner
1.	mpls-pe-noc	Customer - Customer1
2.	mpls1	Customer - Customer1

Rows per page: 10

Go to page: 1 of 1

OK Cancel

Step 4 Choose the policy of choice, then click **OK**.

The MPLS Service Request Editor appears (see [Figure 9-10](#)).

Figure 9-10 MPLS Service Request Editor

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: acme_mgmt_pe_ce

Description:

Showing 0 of 0 records

#	☒	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
Rows per page: 10								

Add Link Delete Link Save Cancel

95379

Step 5 Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields, as shown in [Figure 9-11](#). Notice that the *Select CE* field is enabled. Specifying the CE for the link is the first task required to define the link for this service.

Figure 9-11 Initial Fields Displayed to Define PE-CE Link

#	☐	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	☐	0	Select CE		Select PE		Add	N/A

Rows per page: 10

Add Link Delete Link Save Cancel

95380

Step 6 CE: Click **Select CE**.

The Select CPE Device dialog box is displayed (see [Figure 9-12](#)).

Figure 9-12 Selecting the MCE for the MPLS Link

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	☐	mlce1.cisco.com	AcmeInc	Acme_NY	MANAGED
2.	☐	mlce2.cisco.com	AcmeInc	Acme_NY	MANAGED
3.	☒	mlce8.cisco.com	AcmeInc	Acme_SF	MANAGED_MGMT_LAN
4.	☐	mlce9.cisco.com	AcmeInc	Acme_SF	MANAGED

- From the *Show CPEs with* drop-down list, you can display CEs by *Customer Name*, by *Site*, or by *Device Name*.
- You can use the **Find** button to either search for a specific CE, or to refresh the display.
- You can set the *Rows per page* to **5**, **10**, **20**, **30**, **40**, or **All**.
- This dialog box displays the first page of the list of currently defined CE devices. The number of pages of information is displayed in the lower right corner of the dialog box.

To go to the another page of CE devices, click the number of the page you want to go to.

Step 7 In the **Select** column, choose the name of the MCE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected CE is now displayed in the CE column.

Step 8 *CE Interface*: Choose the CE interface from the drop-down list (see [Figure 9-13](#)).

Figure 9-13 CE and CE Interface Fields Defined

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce8	FastEthernet1/0	Select PE		Add	N/A

Note that in the PE column, the **Select PE** option is now enabled.

Step 9 *PE*: Click **Select PE**.

The Select PE Device dialog box is displayed (see [Figure 9-14](#)).

Figure 9-14 Selecting the PE for the MPLS Link

#	Select	Device Name	Provider Name	Region Name	Role Type
1.	☒	mlpe1.cisco.com	FirstProvider	US	PE_POP
2.	☐	mlpe2.cisco.com	FirstProvider	US	PE_POP
3.	☐	mlpe3.cisco.com	FirstProvider	US	PE_POP
4.	☐	mlpe4.cisco.com	FirstProvider	US	PE_POP

Step 10 In the Select column, choose the name of the PE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.

Step 11 *PE Interface*: Choose the PE interface from the drop-down list (see [Figure 9-15](#)).

Figure 9-15 PE and PE Interface Fields Defined

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce8	FastEthernet1/0	mlpe1	FastEthernet1/0	Add	N/A

Note that the Link Attribute **Add** option is now enabled.

Step 12 In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor is displayed, showing the fields for the interface parameters (see [Figure 9-16](#)).

Figure 9-16 Specifying the MPLS Link Interface Attributes

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	m1pe1
Interface Name *	FastEthernet1/0
Interface Description:	
Shutdown Interface:	☐
Encapsulation:	DOT1Q
Auto-Pick Vlan ID:	☒
CE Information	
CE	m1ce8
Interface Name *	FastEthernet1/0
Interface Description:	
Encapsulation:	DOT1Q

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on each of the PE and CE interface fields, see [Specifying PE and CE Interface Parameters](#), page 5-8.

**Note**

The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both.

- Step 13** Edit any interface values that need to be modified for this particular link, then click **Next**.
The MPLS Link Attribute Editor for the IP Address Scheme appears (see [Figure 9-17](#)).

Figure 9-17 Specifying the MPLS Link IP Address Attributes

MPLS Link Attribute Editor - IP Address Scheme

Attribute	Value
PE-CE Interface Addresses/Mask	
IP Numbering Scheme:	IP Numbered
Extra CE Loopback Required:	☐
Automatically Assign IP Addresses:	☒
IP Address Pool:	Region Pool

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the IP address scheme fields, see [Specifying IP Address Scheme](#), page 5-12.

- Step 14** Edit any IP address scheme values that need to be modified for this particular link, then click **Next**.
The MPLS Link Attribute Editor for Routing Information appears (see [Figure 9-18](#)).

Figure 9-18 Specifying the MPLS Link Routing Protocol Attributes

MPLS Link Attribute Editor - Routing Information	
Attribute	Value
PE-CE Routing Information	
Routing Protocol	BGP
Redistribute Static (BGP only):	☒
Redistribute Connected (BGP only):	☒
CE BGP AS ID *	200 (1-65535)
Neighbor Allow-AS in:	3 (1-10)
Neighbor AS Override:	☐
Redistributed Protocols on CE:	Edit

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the routing information for the PE and CE, see [Specifying Routing Protocol for a Service, page 5-15](#).

Because the service policy used for this service specified the routing protocol as editable, you can change the routing protocol for this service request as needed.

- Step 15** Edit any routing protocol values that need to be modified for this particular link, then click **Next**.
The MPLS Link Attribute Editor for the VRF and VPN attributes appears (see [Figure 9-19](#)).

Figure 9-19 Specifying the MPLS Link VRF and VPN Attributes

MPLS Link Attribute Editor - VRF and VPN	
Attribute	Value
VRF Information	
Export Map:	
Import Map:	
Maximum Routes:	(1-4294967295)
Maximum Route Threshold *	80 (1-100)
VRF Description:	

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the VRF and VPN information, see [Defining the Service Policy VRF and VPN Information, page 5-39](#).

- Step 16** Edit any VRF values that need to be modified for this particular link, then click **Finish**.
You return to the MPLS Service Request Editor.
- Step 17** To save your work on this first link in the service request, click **Save**.
You return to the Service Requests dialog box, where the information for the link you just defined is now displayed (see [Figure 9-20](#)).

Figure 9-20 Service Request for an MPLS Link Completed

Service Requests

Show Services with matching of type

Showing 1-1 of 1 records

#	☐	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	☐	12	REQUESTED	MPLS	ADD	admin	AcmeInc	acme_mgmt_pe_ce	6/19/03 3:33 PM	

Rows per page:

Auto Refresh: ☒

You can add additional links to this service request by choosing **Add Link** and specifying the attributes of the next link in the service. As you can see, the service request is in the *Requested* state. When all the links for this service have been defined, you must deploy the service.

Adding PE-CE Links to the Management VPN

When you have created the Management VPN, then you can proceed to add service for the PE-CE links you want to participate in the Management VPN.

To add PE-CE links, follow these steps:

- Step 1** Navigate to the MPLS Link Attribute Editor - VRF and VPN window for the selected CE.
- Step 2** Check the **Join the management VPN** option, as shown in [Figure 9-21](#).

Figure 9-21 Joining a CE to the Management VPN

MPLS Link Attribute Editor - VRF and VPN

Attribute	Value				
VRF Information					
Export Map:					
Import Map:					
Maximum Routes:	1-4294967295				
Maximum Route Threshold *:	80 (1-100)				
VRF Description:					
Allocate new route distinguisher:	☐				
VRF And RD Overwrite	☐				
Join the management VPN:	☒				
VPN Selection					
PE VPN Membership *:					
Select	Customer	VPN	Provider	CERC	Is Hub
☐	AcmeInc	AcmeIncVPN	FirstProvider	Default	☒

When you join the CE with the Management VPN in this step, ISC generates the appropriate route-map statements in the PE configlet.

The function of the management route map is to allow only the routes to the specific CE into the management VPN. Cisco IOS supports only one export route map and one import route map per VRF (and therefore, per VPN).

Step 3 Complete the service request user interface.
